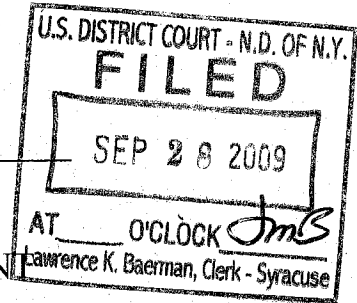


~~SEALED~~ ^{unsealed 9/30/09} ^{SL} United States District Court
NORTHERN DISTRICT OF NEW YORK



UNITED STATES OF AMERICA

CRIMINAL COMPLAINT

FLAY B. ROOD

CASE NUMBER: 5:09-MJ-461 (GHL)

(1)

I, Sgt. Tony Martino, being duly sworn state the following is true and correct to the best of my knowledge and belief:

- (1) In or about June 2009 through August 2009, in Oneida County, in the Northern District of New York, the defendant did:

employ, using, persuading, inducing, enticing or coercing a person under the age of eighteen, to wit: a 3 year old male child, to engage in sexually explicit conduct, for the purpose of producing visual depictions of such conduct, knowing or having reason to know that such visual depictions were produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means;
in violation of Title 18 United States Code, Section(s) 2251(a); and

- (2) In or about June, 2009 through August, 2009, in Oneida County, in the Northern District of New York, the defendant did:

receive visual depictions of minors engaging in sexually explicit conduct using a means and facility of interstate and foreign commerce, that have been transported in and affecting such commerce, and which contain material that has been so transported;
in violation of Title 18 United States Code, Section(s) 2252(a)(2); and

- (3) In or about June, 2009 through August, 2009, in Oneida County, in the Northern District of New York, the defendant did:

possess, and access with intent to view, one or matters which contain visual depictions of a minor or minors engaging in sexually explicit conduct using a means and facility of interstate and foreign commerce, that have been transported in and affecting such commerce, and which contain material that has been so transported;
in violation of Title 18 United States Code, Section(s) 2252(a)(4)(B).

I further state that I am a Sergeant with the Utica, N.Y. Police Department, and that this complaint is based on the following facts:

Continued on the attached sheet and made a part hereof: ☒ YES ☐ NO

Sgt. Tony Martino
Sgt. Tony Martino
Utica, N.Y. Police Department

Sworn to before me, and subscribed in my presence,
September 28, 2009 at
Date

Syracuse, New York

George H. Lowe,
United States Magistrate Judge
Name and Title of Judicial Officer

George H. Lowe
Signature of Judicial Officer

**IN THE UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF NEW YORK**

AFFIDAVIT OF SGT. ANTHONY MARTINO

State of New York)
County of Onondaga).ss:
City of Syracuse)

I, Anthony Martino, having been duly sworn, do hereby state and depose as follows:

1. I am a Sergeant with the Utica, N.Y. Police Department (UPD). I have been with the UPD for over sixteen years and a Sergeant for the past nine years. For the past eight years, I have been a member of the Management Information Systems Unit, and accordingly my duties and responsibilities have included investigations of computer crimes and the forensic examination of digital evidence. Since May 23, 2005, I have been deputized by the United States Marshals Service under their special deputation authority, and as such am authorized to seek and execute federal arrest and search warrants for Title 18 criminal offenses.

2. This affidavit is made in support of an application for a criminal complaint charging Flay B. Rood with violations of (1) Title 18, United States Code, Section 2251(a): employing, using, persuading, inducing, enticing or coercing a person under the age of eighteen, to wit: a 3 year old male child, to engage in sexually explicit conduct, for the purpose of producing visual depictions of such conduct, knowing or having reason to know that such visual depictions were produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means; (2) Title 18, United States Code, Section 2252(a)(2): receiving visual depictions of minors engaging in sexually explicit conduct using a

means and facility of interstate and foreign commerce, that have been transported in and affecting such commerce, and which contain material that has been so transported, and (3) Title 18, United States Code, Section 2252(a)(4)(B): possessing, and accessing with intent to view, one or matters which contain visual depictions of a minor or minors engaging in sexually explicit conduct using a means and facility of interstate and foreign commerce, that have been transported in and affecting such commerce, and which contain material that has been so transported.

3. The statements contained in this affidavit are based on my participation in the investigation of this matter, and on information I have received from other members of the Oneida County Child Advocacy Center, the Oneida County District Attorney's office, and other law enforcement officers with direct knowledge of this investigation. Since this affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that Flay B. Rood has committed violations of Title 18, United States Code, Sections 2251(a), 2252(a)(2), and 2252(a)(4)(B), as outlined above.

Peer-to-Peer Software Programs & Child Pornography

4. Based upon my training and experience as a member of the Internet Crimes Against Children Task Force, I have learned that Peer-to-Peer (P2P) file sharing is a method of communication available to Internet users whereby various computers form a network and use specially designed software programs to access the network. P2P software programs are designed to allow users to trade digital files through a worldwide network that is formed by linking computers together. While there are several P2P networks currently operating, the most predominant network is the Gnutella 1 network. There are several different software

applications (Limewire is an example) that can be used to access the Gnutella 1 network but these applications operate in essentially the same manner.

5. To access a P2P network, a computer user must first install a P2P software package such as Limewire. P2P software programs are publicly available and can be easily downloaded from the Internet. Once installed, a P2P software package allows a computer user to (1) search the P2P network for computer files including picture files and video files that are being "shared" by other members of the network, (2) download digital files, including picture files and video files, that are being shared by other members of the network, and (3) share their respective picture and video files with other members of the P2P network.

6. P2P software programs are used exclusively for the purpose of sharing digital files. When the P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's "shared" folder are available to anyone on the P2P network for download. Conversely, a P2P user is only able to download those computer files that other members of the P2P network have placed in their respective shared folders or files they have individually shared in their saved folder both of which are files that have been authorized for downloading. Most P2P software gives each user a rating based on the number of files that he/she is contributing to the network. This rating can affect the user's ability to download files. The more files a user is sharing, the greater his/her ability is to download some files. This rating system is intended to encourage users to "share" their files, thus propagating the P2P network. However, a user is typically not required to share files to utilize the P2P network.

7. A P2P user obtains files from the P2P network by conducting keyword searches. When a user initially logs onto the P2P network, a list of the files that the user is sharing is transmitted to the network. The P2P software then matches files in these file lists to keyword search requests from other users. A user looking to download files enters one or more keywords

into a search queue that searches all of the other “on-line” P2P users for files that contain the requisite keywords. The results of the keyword search are displayed to the user who then selects file(s) to be downloaded. For example, P2P users who are interested in downloading video and image files containing child pornography will frequently use keyword searches for “PTHC” or “r@ygold” or “Lolita” – terms commonly found in file names of child pornography. Upon executing this keyword search, the computer users P2P program will search the shared files of all other P2P users presently online for files that contain any of these keywords. After the computer performs the keyword search, a list of all responding files containing the keywords will be displayed for the original user.

8. After a file has been selected for download, the downloading process is achieved through a direct connection between the computer requesting the file and various computers hosting the file. Not surprising, at any point in time, multiple computers on a P2P network will be sharing the same file. To expedite the downloading process, a P2P network can (unless the option is disabled by the user) assemble the downloaded file in pieces from various different P2P users who are sharing the requested file. This process of downloading by piecemeal allows a P2P user to download a file from several users in a fraction of the time it would take to download the file from the same user.

9. P2P networks rely on complicated mathematical algorithms to insure that two files are exactly the same. The most common method – and the method used by Limewire – involves a compressed digital representation method known as Secure Hash Algorithm Version 1 or “SHA1”. SHA1 was developed by the National Institute of Standards and Technology (NIST) along with the National Security Agency (NSA) for use within the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS). P2P programs (such as Limewire) use the SHA1 algorithm to assign a digital signature to each file which is comprised of a

sequence of numbers and letters. This digital signature, or SHA1 value, is the fingerprint (very much akin to DNA) for a digital file.

10. By comparing the SHA1 values of two files, one can conclude that two files are or are not the same with a precision that greatly exceeds 99.9999 percent certainty. I am aware of no documented occurrences of two different files being found on the Internet having different content while sharing the same SHA1 value. The use of SHA1 values to match movies and images has proven to be extremely reliable.

11. As P2P networks and software programs rely on SHA1 values (and not file names) for purposes of facilitating the downloading process, the SHA1 value of each file placed in a P2P user's "shared" folder is calculated each time the user opens the P2P file sharing software. By the time a P2P user's shared files are subject to keyword search and download by other P2P network participants, the SHA1 values for all of the user's shared values have already been calculated.

12. The search feature in a P2P network also relies on SHA1 values. For example, a P2P search for suspect child pornography using a "PTHC" search query will result in a list of SHA1 digital signatures (with file names that have PTHC in the name) that can be downloaded. By using the SHA1 values in conjunction with the search function of P2P, your affiant has compared the SHA1 values of hundreds of suspect images of child pornography identified through undercover searches of the P2P network with SHA1 values known to belong to movies or images of child pornography.

Peer Spectre & Child Pornography Investigations

13. Your affiant has received training and experience in using computer programs developed by law enforcement that are known as Limewire EP2P and "Peer Spectre." Peer Spectre performs automated searches of P2P networks in search of suspect child pornography

that is being offered by users for downloading to the public. Peer Spectre uses the results of these automated searches to identify IP addresses that are sharing suspect child pornography. In addition to collecting and storing the IP addresses, Peer Spectre collects and reports the file names and corresponding SHA1 values of the images of suspect child pornography, and also the date and time in which the suspect child pornography was being offered for downloading by the corresponding IP address.

14. The operation of the Peer Spectre computer program – including the search for child pornography and the collection of data regarding the IP addresses and the files that contain the suspect child pornography – is systematic and relies on the same processes each time the computer program is operated. All of the information collected by Peer Spectre is publicly available information that can be identified by any computer user using easily-accessible computer software.

Details of the Investigation

15. On August 17, 2009, your affiant used the Limewire EP2P and Peer Spectre programs to investigate, in an undercover capacity on a P2P network, computers with New York IP addresses that were or had been sharing child pornography on the Internet, looking for IP addresses that were actively sharing child pornography within New York State, and specifically in Oneida County.

16. On August 17, 2009, IP address 67.249.48.12 was identified by the Peer Spectre automated software program as having offered suspect child pornography for downloading over 40 times between the dates of June 15, 2009 and August 8th, 2009.

17. Your affiant noted the date/time, SHA1 Digital Signature, and file names as reported by Peer Spectre as advertised by the computer located at IP address 67.249.48.12 and three of them are as follows:

A) DATE & TIME
07/08/2009 at 20:14:49 GMT

SHA1 DIGITAL SIGNATURE
KGE CXAOYTCCYYIDB5EPZQN2UZJ4EHUYR

FILE NAME
"r@ygold - pedo - 13yo brother fucks 11yo sister and sperm inside 61 943 812.mpg"

B) DATE & TIME
08/08/2009 AT 03:57:05 GMT

SHA1 DIGITAL SIGNATURE
57RSE27JFMUDB4TDF2YOSBTTWSNYTY2V

FILE NAME
"Aaaaaaaa [Brazilian] 8yo boy butt-fucks 11yo girl [see @01min06sec] pthc-!!-NEW!!-Neighborhood Kids - 10yrs buffing 04-01-2005.mpg"

C) On the following date/time, using the Limewire EP2P software, a browse host was successfully completed with the client at IP address 67.249.48.12. The following file was partially downloaded, but not in sufficient quantity to be viewable.

DATE & TIME
07/08/2009 17:30 EDT

SHA1 DIGITAL SIGNATURE
CTOSIVKLQZQYLTHWP7HZV7LTVLYO6SOK

FILE NAME
"5yo Girl Raped By Daddy - Preteen - Child Pornography - Illegal - PTHC - Pedo - R@ygold - Babyshivid - KDQuality - Zadoom - Lolita - QWERTY - ChildFugga - Ddoggprn (1).mpg"

18. Because filenames do not always accurately depict the contents of the file, your affiant compared the following SHA1 values with files recovered in previous investigations that contain identical SHA1 values. Your affiant has watched each of the video files corresponding to these SHA1 values and describes the content of each video as follows:

A. Sha1 Value: KGE CXAOYTCCYYIDB5EPZQN2UZJ4EHUYR

Description: This is a video that is approximately 5:55 long. The video starts by showing a prepubescent female lying on her back wearing only underwear, which is then removed by an unknown subject. The video shows the female being digitally penetrated. The video cuts to another scene and shows an adult male having sexual intercourse with the female

B. SHA1 Value: CTOSIVKLQZQYLTHWP7HZV7LTVLYO6SOK

Description: This video shows a female, with dark hair, who appears to be less than 16 years old. During the course of this video, the female strips off her clothes and performs oral sex on a male.

19. Subsequently, a subpoena was issued to obtain subscriber information for IP Address 67.249.48.12 for the date/time that your affiant successfully connected to the P2P client and was able to partially download the video file described in section 18C above. Pursuant to the subpoena response, it was determined that an identified person with the last name Rood, of a Utica, NY address was assigned IP Address 67.249.48.12 on the aforementioned date/time.

Search Warrant

20. On August 28, 2009, Hon. Barry Donalty, Oneida County Judge, issued a search warrant for the Utica residence listed on the subpoena response, authorizing a search of the residence and electronic media found therein for items evidencing violations of New York State Penal law section 263 (distributing, receiving, or possessing child pornography). That warrant was executed by law enforcement officers on August 31, 2009.

21. **Flay Rood** was present during the search warrant, and agreed to be interviewed. Inv. Jeremy Vanhorne of the Utica Police Department interviewed **Flay Rood**, during which **Rood** admitted that he has been receiving child pornography over the Internet, including through peer to peer file sharing, and that he had saved images and videos of child pornography on to his computer hard drive and his thumb drive.

22. As a part of the execution of the search warrant, UPD Officer Edin Selimovic

performed a forensic preview of a computer hard drive located within the residence. During Officer Selimovic's preview, he located image and video files containing child pornography. Officer Selimovic saved two video files and two still images from the computer, to compact disk. I have reviewed the contents of the disk, which are available for the Court's review upon request.

- a. One of the videos found the computer, entitled "#(Pthc) 9Yo Jenny Blows Dad & Dog.mpg" is a 16 minute video compilation showing a prepubescent female child engaged in various activities including the lewd and lascivious exhibition of her genitals, bondage of her legs while she is penetrated by an adult's finger, and performing oral sex on an adult male.

- b. One of the still images found on the computer, entitled "8yo preteen girl raped by 16yo brother, sister tight virgin pedo pussy, r2ygold, inzest, incest, taboo, girl, girls, hot schoolteens.net porn fine picture (2).jpg" is a still image file depicting a pre-pubescent girl, whose age appears consistent with the "8 Yo" of the title, the girl's legs are spread exposing her vagina and a male is seen placing his penis against her vagina.

23. As part of the forensic examination of the evidence seized from the house of Flay Rood, your affiant identified 17 images that were located on a thumb drive. These images depict two separate pre-pubescent males displaying and touching their penises. In some of the images, an adult male's body is seen and he is shown pulling the young boy's underwear aside to display their penis. One of the pre-pubescent males seen in these pictures has been since identified and is known to have been 3 years old at the time the image was taken. Investigation has revealed that the 3 year old child is known to Flay Rood. The second pre-pubescent male has not been identified as of the writing of this affidavit.

24. As part of the investigation in to the identity of the adult male seen in the images found on the thumb drive, Investigator Patrick O'Connor of the Oneida County District

Attorney's office was issued a search warrant signed by Hon. Barry Donalty, Oneida County Judge, that authorized the searching and photographing of the body of Flay Rood, as well as the seizure of articles of clothing seen being worn by the adult male in the images. Subsequently, the adult male was identified as Flay Rood through comparison of unique physical markings on the body and matching articles of clothing that were seized pursuant to the search warrant.

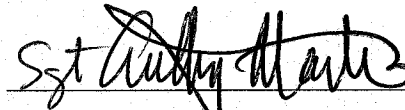
25. The forensic examination of the images from the thumb drive showed that EXIF data¹ was present in all of the images. The EXIF data contained within these images confirms that the images were taken with a LG cellular telephone model "Fusic" in 2008. The children depicted in these images are pre-pubescent males. The child that has been identified is currently 4 years old, and was 3 years old when the picture was taken. The images depict the lewd and lascivious exhibition of both children's penises. Additionally, in some of the pictures the child is sitting on an adult's lap, the adult is pulling the child's underwear aside to expose the genitals, and the child is touching his penis in a manner consistent with masturbation. These and all of the images of the children are available for the Court's inspection upon request.

26. As a part of the investigation, it was learned that the LG model phone utilized to capture the digital images was no longer possessed by the suspect. Witness interviews confirmed that the suspect had previously possessed a cellular phone of the make and model used to take the images. A search of records filed by LG with the U.S. Federal Communications Commission show that the LG Fusic cellular phone was manufactured in Korea. As such, it is a material that has been transported in interstate and foreign commerce.

Conclusion

¹ Digital cameras save JPEG (.jpg) files with EXIF (Exchangeable Image File) data. Camera settings and scene information are recorded by the camera into the image file. Examples of stored information are shutter speed, date and time, focal length, exposure compensation, metering pattern and if a flash was used.

27. Based upon the above information, I believe that there is probable cause to believe that Flay Rood (1) has employed, used, persuaded, induced, enticed and coerced a person under the age of eighteen, to wit: a 3 year old male child, to engage in sexually explicit conduct, for the purpose of producing visual depictions of such conduct, knowing or having reason to know that such visual depictions were produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, in violation of Title 18, United States Code, Section 2251(a); (2) knowingly received visual depictions of minors engaging in sexually explicit conduct using a means and facility of interstate and foreign commerce, that have been transported in and affecting such commerce, and which contain material that has been so transported, in violation of Title 18, United States Code, Section 2252(a)(2); and (3) knowingly possessed and accessed with intent to view, one or matters which contain visual depictions of a minor or minors engaging in sexually explicit conduct using a means and facility of interstate and foreign commerce, that have been transported in and affecting such commerce, and which contain material that has been so transported, in violation of Title 18, United States Code, Section 2252(a)(4)(B).

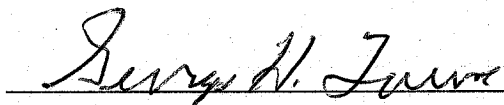


Sgt. Tony Martino,

Utica, N.Y. Police Department

Sworn to me this

28th day of September, 2009



George H. Lowe

United States Magistrate Judge